



**Merchant Integration Guide**  
**Ecommerce**

**KINA BANK LIMITED**  
**ECOMMERCE MERCHANT INTEGRATION GUIDE**

**Version 2.0**



## Merchant Integration Guide Ecommerce

### Document Information

Prepared By : Kina Bank Limited

Document Version No : 2.0

Document Version Date : 02 Jun 2022

### Version History

Ver. No.	Ver. Date	Revised By	Remarks
1.0	23 Jun 2020	Tan Kah Hoe	
1.1	24 Jun 2020	Tan Kah Hoe	Switch term "checkout page" to "order confirmation page" Add section for MAC Calculation
1.2	29 Jun 2020	Tan Kah Hoe	Reshuffle MAC source string order Secret Key for HMAC Testing in TEST environment
1.3	30 Jun 2020	Tan Kah Hoe	List of Action Code in Response List of EGW Response Code (RC)
1.4	07 May 2021	Tan Kah Hoe	Check Transaction request and response
1.5	14 May 2021	Tan Kah Hoe	Include Merchant Test Data (test card, terminal)
1.6	28 Jul 2021	Tan Kah Hoe	Hosted payment page, Embedded payment page Digital Signature for response
1.7	06 Sep 2021	Tan Kah Hoe	Subdomain name change – <a href="https://ipg.kinabank.com.pg/">https://ipg.kinabank.com.pg/</a>
1.8	14 Apr 2022	Tan Kah Hoe	Check Transaction request and response in JSON format Online HMAC calculator
1.9	09 May 2022	Tan Kah Hoe	Switch order, make Embedded Payment Page precede Hosted Payment Page Add JS example code for calculating Hmac
2.0	02 Jun 2022	Tan Kah Hoe	Digital signature in response: outline formatting rules to amount field (2 decimal point)



## Merchant Integration Guide Ecommerce

### Table of Contents

<b>Introduction .....</b>	<b>3</b>
<b>Transaction Flows.....</b>	<b>3</b>
<b>Authorization Request .....</b>	<b>4</b>
<b>Authorization Response .....</b>	<b>5</b>
<b>Reversal Request.....</b>	<b>6</b>
<b>Reversal Response.....</b>	<b>6</b>
<b>Check Transaction request .....</b>	<b>7</b>
<b>Check Transaction Response .....</b>	<b>8</b>
<b>Check Transaction request – JSON .....</b>	<b>9</b>
<b>Check Transaction response – JSON .....</b>	<b>9</b>
<b>Payment Page Integration.....</b>	<b>10</b>
<b>Embedded Payment Page integration guide .....</b>	<b>11</b>
<b>Hosted Payment Page integration guide .....</b>	<b>12</b>
<b>Digital Signature .....</b>	<b>13</b>
<b>Secret key.....</b>	<b>13</b>
<b>MAC source string.....</b>	<b>13</b>
<b>Digital Signature in Request .....</b>	<b>14</b>
<b>Digital Signature in Response.....</b>	<b>15</b>
<b>EGW Response Code .....</b>	<b>16</b>
<b>Test Data.....</b>	<b>17</b>
<b>Online HMAC Calculator.....</b>	<b>18</b>



## Introduction

This document illustrates the steps to integrate merchant e-commerce site to Kina Payment Gateway. Kina Payment Gateway support the acceptance of the following Card brands:

1. Visa
2. MasterCard
3. Union Pay
4. Kina Debit Card
5. ANZ Debit Card
6. Mibank Debit Card

## Transaction Flows

### 1. Checkout Page

After selecting good and services, customer proceed to checkout page to fill in delivery info.

### 2. Order confirmation page.

Upon finalizing delivery info, customer click a button and merchant site display order confirmation page and present payment method to customer.

### 3. Kina Payment Page iframe

In order confirmation page, customer choose to pay by credit/debit card. **Order confirmation page** must include a HTTP FORM element that contains INPUT or HIDDEN fields (complete set of fields described in next section) required to authorize the transaction, submit HTML FORM to iframe, FORM target=[https://devegateway.kinabank.com.pg/cgi-bin/cgi\\_link](https://devegateway.kinabank.com.pg/cgi-bin/cgi_link).

6.1 A page to collect credit card details (hosted by Kina Bank Limited) will be displayed as overlay iframe on top of order confirmation page

### 4. Customer click pay

In Kina Payment Page iframe, customer fill in card number and other card details, and click pay. Kina payment gateway receive the authorization request and validates request information including the message authentication code (MAC). If the request fails, gateway sends an error response back to merchant system.

### 5. Cardholder authentication.

If the provided card number belongs to a card range with a defined cardholder authentication method, gateway calls the corresponding authentication module like 3-D Secure, which performs protocol-specific processing like One Time Password. If cardholder authentication is unsuccessful, Gateway returns an error message to the merchant system.

### 6. Transaction authorization

Gateway sends an authorization request to Kina card system. Upon authorization, reception gateway prepares and sends a transaction response back to the merchant system. If authorization is successful, the response message will contain "Internal Reference Number" field, to be used by the merchant system so it can reverse/refund the obtained authorization without the credit card information.



## Merchant Integration Guide Ecommerce

### Authorization Request

Following fields set will be posted to Kina Payment Gateway through HTTP POST method. These fields can be rendered as HTML INPUT or HIDDEN elements in order confirmation page. Merchant site should perform basic prevalidation to ensure the values conform to the below requirements

Field	Size	Description
AMOUNT	1-12	Order amount in float format with decimal point separator, up to 2 decimal point. Example: <b>98.30</b>
CURRENCY	03	Order currency: 3-character currency code
ORDER	6-20	Merchant order ID, numeric. Last 6 digits used as a system trace audit number, which must be unique within a day for the terminal id.
DESC	1-50	Order description
MERCH_NAME	1-50	Merchant name (recognizable by cardholder)
MERCH_URL	1-250	Merchant primary web site URL
MERCHANT	15	Merchant ID assigned by bank
TERMINAL	8	Merchant Terminal ID assigned by bank
EMAIL	80	E-mail address for notification. If this field is present Gateway may send transaction results notification to specified e-mail address
TRTYPE	2	Must be equal to "1" (Retail Financial Request).
COUNTRY	02	Merchant shop 2-character country code. Must be provided if merchant system located in a country other than the gateway server's country.
MERCH_GMT	1-5	Merchant UTC/GMT time zone offset (e.g. -3). Must be provided if merchant system located in a time zone other than the gateway server's time zone.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between merchant server and e-Gateway server must not exceed 1 hour, otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
BACKREF	1-250	Merchant URL for posting authorization result.
P_SIGN	1-256	Merchant MAC in hexadecimal form.



## Merchant Integration Guide

### Ecommerce

## Authorization Response

Kina Payment Gateway processes the authorization request and returns the response to merchant URL provided in the **BACKREF** incoming field. Additionally, the same field set may be sent to the merchant via to the email address provided in the **EMAIL** incoming field.

Field	Size	Description
TERMINAL	8	Echo from the request
TRTYPE	2	Echo from the request
ORDER	6-20	Echo from the request
AMOUNT	12	Amount authorized. Usually, will be equal to original amount plus acquirer fee.
CURRENCY	3	Echo from the request
ACTION	1	E-Gateway action code: 0 – Transaction successfully completed; 1 – Duplicate transaction detected; 2 – Transaction declined; 3 – Transaction processing fault; 4 – Information message.
RC	02	Transaction response code (ISO-8583 Field 39)
APPROVAL	06	Client bank's approval code (ISO-8583 Field 38). Can be empty if not provided by card management system.
RRN	12	Merchant bank's retrieval reference number (ISO-8583 Field 37).
INT_REF	1-32	E-Commerce gateway internal reference number
TIMESTAMP	14	E-Commerce gateway timestamp in GMT: YYYYMMDDHHMMSS
NONCE	1-64	E-Commerce gateway nonce value. Will be filled with 8-32 unpredictable random bytes in hexadecimal format. Will be present if MAC is used.
P_SIGN	1-256	E-Commerce gateway MAC (Message Authentication Code) in hexadecimal form. Will be present if MAC is used.



## Merchant Integration Guide

### Ecommerce

## Reversal Request

The reversal transaction request shall be sent by the merchant system Kina Payment Gateway to cancel previously authorized or completed transactions.

All fields are provided by merchant system and the cardholder does not participate in this transaction.

Field	Size	Description
ORDER	6-20	Merchant order ID from request.
AMOUNT	12	Transaction amount. Float format with decimal point separator.
CURRENCY	3	Currency name. Must be the same as in authorization response.
RRN	12	Retrieval reference number from authorization response.
INT_REF	1-32	Internal reference number from authorization response.
TRTYPE	2	Must be equal to "24" (Reversal Request).
TERMINAL	8	Merchant terminal ID assigned by bank. Must be equal to "TERMINAL" field from authorization request.
TIMESTAMP	14	Merchant transaction timestamp in GMT: YYYYMMDDHHMMSS. Timestamp difference between Internet shop and e-Gateway must not exceed 1 hour otherwise e-Gateway will reject this transaction.
NONCE	1-64	Merchant nonce. Must be filled with 8-32 unpredictable random bytes in hexadecimal format. Must be present if MAC is used.
P_SIGN	1-256	Merchant MAC in hexadecimal form.

## Reversal Response

Gateway processes a reversal request and returns the result fields to the merchant system within a response document. Response fields and format are the same as for the [authorization response](#).



## Merchant Integration Guide

### Ecommerce

#### Check Transaction request

Following fields set will be posted to Kina Payment Gateway through HTTP POST method. These fields can be rendered as HTML INPUT or HIDDEN. Merchant site should perform basic prevalidation to ensure the values conform to the below requirements

Field	Size	Description
ORDER	6-20	Original Transaction Order ID
TERMINAL	8	Merchant Terminal ID assigned by bank
TRTYPE	2	Must be equal to "90" (Request Status).
TRAN_TRTYPE	2	Original Transaction TRTYPE. Must be equal to "1" (Retail Financial Request)
P_SIGN	1-256	Merchant MAC in hexadecimal form.





## Merchant Integration Guide Ecommerce

### Check Transaction Response

A HTML page will be returned with the transaction status information

#### Example: declined transaction

Action code:	3
Response code:	-19
Transaction status message:	Authentication failed
Terminal:	99999001
Card number:	5200XXXXXXXXX0000
Transaction amount:	0.1
Transaction currency:	PGK
Transaction state:	5
Merchant order id:	1620370035
Original transaction type:	1
Timestamp:	20210507071827
Nonce:	F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0
Transaction signature:	5DCA0448E3B7A2233EB0E4301AF82184FC480B94B161D33BD5AEC2981CCB4588

#### Example: Approved transaction

This is the transaction summary information

Action code:	0
Response code:	00
Transaction status message:	Approved
Terminal:	99999001
Card number:	4012XXXXXXXXX3010
Transaction amount:	0.1
Transaction currency:	PGK
Transaction date:	2021.05.07 17:35:47
Transaction state:	3
Merchant order id:	1620372924
Your bank's approval code:	082754
Transaction reference with the merchant's bank:	112701806186
Internal transaction reference:	18768BA3DBF9634F
Original transaction type:	1
Timestamp:	20210507073602
Nonce:	F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0
Transaction signature:	C26A7602C5D3D954E3DF41E1D0752D72C50A9FCC47C039869087E75E4BCA9A0A



## Check Transaction request – JSON

Check Transaction request can be sent as JSON format.

JSON request must be sent to following URI

[https://devegateway.kinabank.com.pg/cgi-bin/cgi\\_json](https://devegateway.kinabank.com.pg/cgi-bin/cgi_json)

Content-Type = application/json;

Please be aware that when sending JSON request, certain fields are named differently, please refer to following examples:

```
{
  "trtype": "90",
  "terminal": "99999001",
  "trTypeReq": "1",
  "orderId": "1649833399",
  "timestamp": "20220414050320",
  "merchGmt": "-480",
  "nonce": "F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0",
  "signature": "6ad2ce527c98a5b291adbd5c1db28a435aae4738c703b1dcc879a13e8e9ee2ed"
}
```

## Check Transaction response – JSON

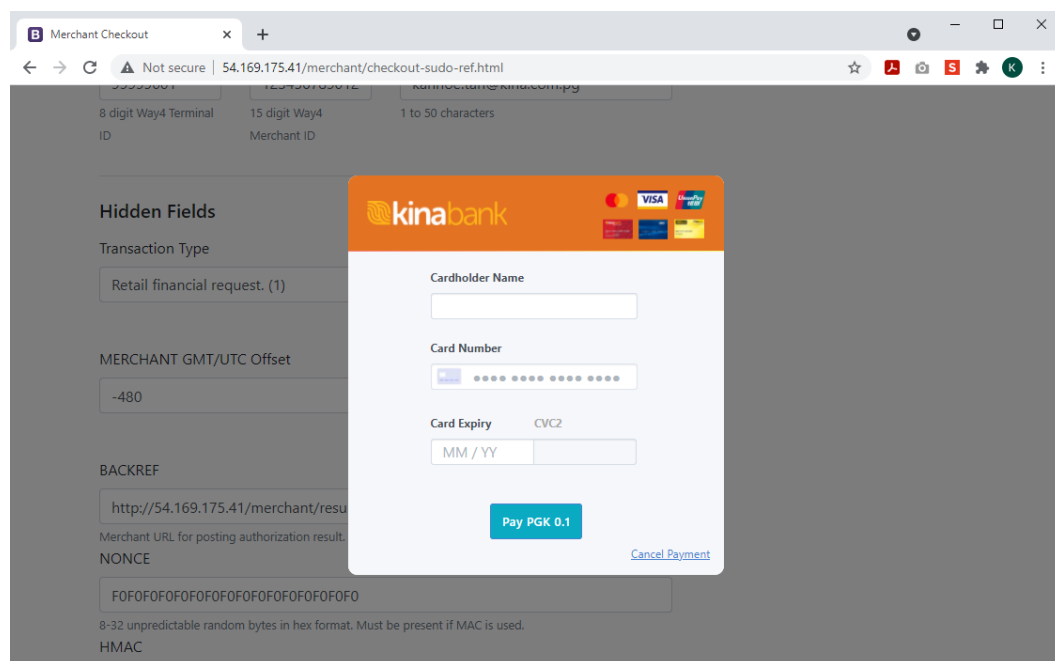
When sending a JSON request, the gateway will return response in JSON format. Example:

```
{
  "terminal": "99999001",
  "actionCode": "0",
  "responseCode": "00",
  "statusMsg": "Approved",
  "amount": "12.34",
  "currency": "PGK",
  "tranDate": "2022.04.13 17:04:50",
  "rrn": "210301927407",
  "intRef": "A642FA9F4F76F565",
  "nonce": "f000c202682f35c8f20730548ace2e69",
  "signature": "6AD2CE527C98A5B291ADB5C1DB28A435AAE4738C703B1DCC879A13E8E9EE2ED",
  "timestamp": "20220414050320"
}
```

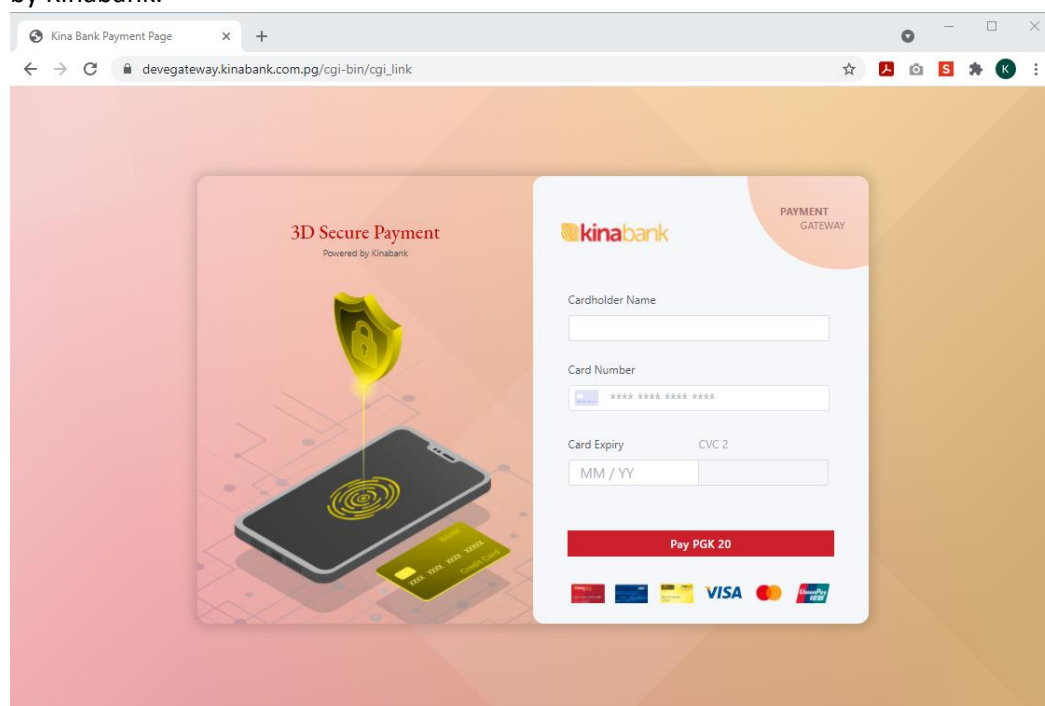
## Payment Page Integration

Kinabank supports 2 types of payment page.

**Embedded Payment Page** displays the payment form as overlay (iframe) to the checkout page. consumer stays on the merchant site rather than being redirected to a separate site.



**Hosted Payment Page** redirect the consumer from your shop to a standalone payment page hosted by Kinabank.





## Merchant Integration Guide Ecommerce

### Embedded Payment Page integration guide

In the `<head>` of order confirmation page

```
<head>
  <meta http-equiv="Cache-Control" content="no-cache, no-store, must-revalidate" />
  <meta http-equiv="Pragma" content="no-cache" />
  <meta http-equiv="Expires" content="0" />
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <script src="https://devegateway.kinabank.com.pg/kina/js/kbl-ec.js"></script>
  <link href="https://devegateway.kinabank.com.pg/kina/css/kbl-ec.css" rel="stylesheet">
</head>
```

In production environment, substitute test domain `devegateway.kinabank.com.pg` with production domain `ipg.kinabank.com.pg`

**Cache-Control, Pragma and Expires** meta tag ensure the page and its content are not cached, use of these meta elements are strongly recommended, these directive will ensure the browser to fetch a fresh copy of the page resources (CSS, JS and Images) from the server rather than using the cache version, which may be outdated.

**Viewport** meta tag, it's recommended to use this tag for fluid and responsive design that looks good in both desktop and mobile

**kbl-ec.js** and **kbl-ec.css** are mandatory javascript and css to support the functions and the look and feel of the payment page integration, its recommended to append some random number like timestamp to prevent caching, example: `kbl-ec.js?202109061545123`

In the `<body>` of order confirmation page

```
<body>
  <form id="kblPaymentForm" method="POST" target="kblpaymentiframe">
    <input type="text".../>
    <input type="hidden".../>
    ...
  </form>

  <button type="button" onclick="submitPaymentForm2()" > Pay by Cards</button>

  <div id="kbliframediv" class="kbliframeoverlay">
    <div id="kbliframeinnerdiv">
      <iframe id="kblpaymentiframe" name="kblpaymentiframe"></iframe>
    </div>
  </div>
</body>
```

**<FORM>** tag should enclose all the INPUT fields described in [Authorization Request](#), it's advisable to disable the edit of all fields in order confirmation page and the MAC is precalculated in the P\_SIGN fields.

**<Button>** "onclick" event call the javascript `submitPaymentForm2()` to invoke and make the iframe visible. It's recommended for the merchant site to perform prevalidation before displaying the order confirmation page so the values in the INPUT/HIDDEN elements conform to the requirements of Kina Payment Gateway.



## Merchant Integration Guide Ecommerce

### Hosted Payment Page integration guide

In your checkout confirmation page, submit the HTML form to the following URL

#### **Test**

```
<form id="kblPaymentForm" action="https://devegateway.kinabank.com.pg/cgi-bin/cgi_link" method="POST">
```

#### **Production**

```
<form id="kblPaymentForm" action="https://ipg.kinabank.com.pg/cgi-bin/cgi_link" method="POST">
```



## Merchant Integration Guide Ecommerce

### Digital Signature

To safeguards against man-in-the-middle attacks, it's mandatory to implement digital signatures for all request and response message.

Digital signature is a mathematical scheme to verify the authenticity of message exchanged between two nodes. A valid digital signature lets a recipient know the message was created by a known sender, and that it was not altered while transmitting.

Kina Payment Gateway employs Hash-based Message Authentication Code (HMAC) as a form of digital signature. HMAC involves the use a cryptographic key (secret key) in conjunction with a hash function

### Secret key

A secret key is used to generate/verify the HMAC.

For integration test, use the secret key defined in [Test Data](#) section of this document. Please liaise with your bank representative to obtain secret key for production live system.

### MAC source string

The fields used to generate digital signatures are defined in the following table

TRTYPE	MAC Fields for Request	MAC Fields for Response
1 – Retail Financial Request	TERMINAL TRTYPE AMOUNT CURRENCY ORDER MERCHANT EMAIL BACKREF TIMESTAMP MERCH_NAME COUNTRY MERCH_URL MERCH_GMT DESC NONCE	ACTION RC APPROVAL CURRENCY AMOUNT <i>*Please format the returned amount with decimal point (2 decimal point)</i> TERMINAL TRTYPE ORDER RRN MERCHANT TIMESTAMP INT_REF NONCE
24 – Reversal Request	ORDER	ORDER
90 – Check Transaction Status	ORDER	ORDER



## Merchant Integration Guide Ecommerce

### Digital Signature in Request

To generate a digital signature, merchant system must assemble a MAC source string according to the above tables. All field values are prefixed with the decimal field length in ASCII and concatenated in exact same order defined in the above table. If the field is not present, the '-' character is added to the message in its place.

Suppose we have a transaction of following values

Field	Length	Value
TERMINAL	8	99999999
TRTYPE	1	1
AMOUNT	5	11.48
CURRENCY	3	USD
ORDER	6	771446
MERCHANT	15	123456789012345
EMAIL	19	pgw@mail.sample.com
BACKREF	33	https://www.sample.com/shop/reply
TIMESTAMP	14	20030105153021
MERCH_NAME	17	Books Online Inc.
COUNTRY	0	
MERCH_URL	14	www.sample.com
MERCH_GMT	0	
DESC	16	IT Books. Qty: 2
NONCE	16	F2B2DD7E603A7ADA

#### MAC source string for the above example:

89999999911511.483USD67714461512345678901234519pgw@mail.sample.com33https://www.sample.com/shop/reply142003010515302117Books Online Inc.-14www.sample.com-16IT Books. Qty: 216F2B2DD7E603A7ADA

After the MAC source string is assembled, the merchant system must apply a cryptographic algorithm to generate the message authentication code. The default algorithm is **HMAC\_SHA256**.

Below is an example how to implement this using JS.

#### JavaScript Examples

```
let macSourceString =  
'89999999911511.483USD67714461512345678901234519pgw@mail.sample.com33https://www.sample.com/shop/reply142003010515302117Books Online Inc.-14www.sample.com-16IT Books. Qty: 216F2B2DD7E603A7ADA';  
  
const secret = 'debdd135e436905c7a02f20c56c83a4c501adf555457f0df';  
let txtKey = CryptoJS.enc.Hex.parse(secret);  
let encryptedMac = CryptoJS.HmacSHA256(macSourceString, txtKey);
```

Encrypted MAC should be sent in "P\_SIGN" field, value can be either upper case or lower-case hexadecimal string.



### Digital Signature in Response

Digital signature is stored in “P\_SIGN” field in response message.

To verify the authenticity of the response message. Merchant’s system must compute a digital signature by employing the same method described above.

1. First assemble the MAC source string from the response.
2. Apply HMAC\_SHA256 algorithm and compare the result with the P\_SIGN values returned by payment gateway.





## Merchant Integration Guide Ecommerce

### EGW Response Code

RC	Description
-1	A mandatory request field is not filled in
-2	CGI request validation failed
-3	Acquirer host (NS) does not respond or wrong format of e-gateway response template file
-4	No connection to the acquirer host (NS)
-5	The acquirer host (NS) connection failed during transaction processing
-6	e-Gateway configuration error
-7	The acquirer host (NS) response is invalid, e.g. mandatory fields missing
-8	Error in the "Card number" request field
-9	Error in the "Card expiration date" request field
-10	Error in the "Amount" request field
-11	Error in the "Currency" request field
-12	Error in the "Merchant ID" request field
-13	The referrer IP address (usually the merchant's IP) is not the one expected
-14	No connection to the iPOS PINpad or agent program is not running on the iPOS computer/workstation
-15	Error in the "RRN" request field
-16	Another transaction is being performed on the terminal
-17	The terminal is denied access to the e-Gateway
-18	Error in the CVC2 or CVC2 Description request fields
-19	Error in the authentication information request or authentication failed.
-20	A permitted time interval (1 hour by default) between the transaction Time Stamp request field and the e-Gateway time is exceeded
-21	The transaction has already been executed
-22	Transaction contains invalid authentication information
-23	Invalid transaction context
-24	Transaction context data mismatch
-25	Transaction canceled (e.g. by user)
-26	Invalid action BIN
-27	Invalid merchant name
-28	Invalid incoming addendum(s)
-29	Invalid/duplicate authentication reference
-30	Transaction was declined as fraud
-31	Transaction already in progress
-32	Duplicate declined transaction
-33	Client authentication by random amount or verify one-time code in progress
-34	MasterCard Installment client choice in progress
-35	MasterCard Installments auto canceled

## Test Data

Following test data can be used to perform integration testing with KINA PAYMENT GATEWAY in test environment.

### Test Card

Card Type	Card Attributes
Visa Card	4012000000003010 Expiry: 12/27 or any future date CVV: 123
Kina Debit Card	5076480200021147 Expiry: 03/24

### Test Merchant

Field	Value
TERMINAL	999999001
MERCHANT	000000099999001

### Secret Key

debdd135e436905c7a02f20c56c83a4c501adf555457f0df

**“ Please ensure Secret Key data type is set to HEX ”**




## Merchant Integration Guide Ecommerce

### Online HMAC Calculator

A good reference site for HMAC testing.

<https://www.liavaag.org/English/SHA-Generator/HMAC/>



**På norsk**

**GENERATORS**

[MD4 and MD5 Generator](#)

[SHA generator](#)

**GENERATORS**

- ✓ HMAC
- ✓ SHA3-512
- ✓ SHA3-384
- ✓ SHA3-256
- ✓ SHA3-224
- ✓ SHA-512
- ✓ SHA-384
- ✓ SHA-256
- ✓ SHA-224
- ✓ SHA-1
- ✓ MD5
- ✓ MD4

### ONLINE HMAC GENERATOR

Here is an HMAC (keyed-hash message authentication code) online generator that generates a cryptographic hash function in combination with a secret encryption key.

Hash Encryption Generator

**Input**

**Input Type**

TEXT

**Key**

**Key type**

HEX

**SHA variant**

SHA-256

**Output type**

HEX

**Result**

**HMAC** 6ad2ce527c98a5b291adbd5c1db28a435aae4738c703b1dcc879a13e8e9ee2ed

**Copy** **Reset**